ΤΕΙ ΗΠΕΙΡΟΥ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε
ΜΕΤΑΠΤΙΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

Ασφάλεια

ΛΙΑΓΚΟΥ ΒΑΣΙΛΙΚΗ
ΔΙΑΛΕΞΗ-Ι

Μηχανισμοί Ασφάλειας - 1η Θεώρηση

Πρόληψη

Φυσική ασφάλεια, access control, replication, Firewalls, Κρυπτογράφηση, Ψηφ. Υπογραφή, Προγράμματα antivirus, Ασφαλής Προγραμματισμός, Πολιτική κωδικών ασφάλειας,…

Ανίχνευση

Συστήματα Ανίχνευσης Εισβολών (IDS), Αρχεία καταγραφής, penetration testing,…

Απόκριση

Back-up, Digital forensics, malware removal, hot sites,…

Μηχανισμοί Ασφάλειας - 2η Θεώρηση*

NIST 800-100 I.S. Handbook: A Guide for Managers

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 11-1: Security Control Class, Family, and Identifier

Κατηγορία Ελέγχου`	Πρόληψη	Ανίχνευση	Αντιμετώπιση
Φυσικής πρόσβασης (παραδείγματα)			
Φράχτες	X		X
Προσωπικό Ασφαλείας	X	X	X
Έξυπνες Κάρτες (smartcards), Βιομετρία	X		
Διαχειριστικός (παραδείγματα)			
Πολιτικές Ασφάλειας	X	X	X
Έλεγχος και Εποπτεία	X	X	
Εκπαίδευση υπαλλήλων	X	X	X
Λογικής Πρόσβασης (παραδείγματα)			
Λίστες Ελέγχου Πρόσβασης (ACLs), MAC, RBAC,…	X		
Passwords, CAPTCHAs	X		
Λογισμικό Antivirus, Anti-spam, Anti-Spyware,..	X	X	X
Κρυπτογράφηση Δεδομένων και Επικοινωνιών	X	X	
Firewalls (Packet Filters, Application Gateways)	X	X	
Συστήματα Ανίχνευσης & Αποτροπής Εισβολών (IDS/IPS)	X	X	X

http://www.cs.uwf.edu/~rdavid/CEN4540/sec3.ppt

D. Το Γνωστικό Αντικείμενο – 1η Θεώρηση

Model A for Security (Stallings, 2010)

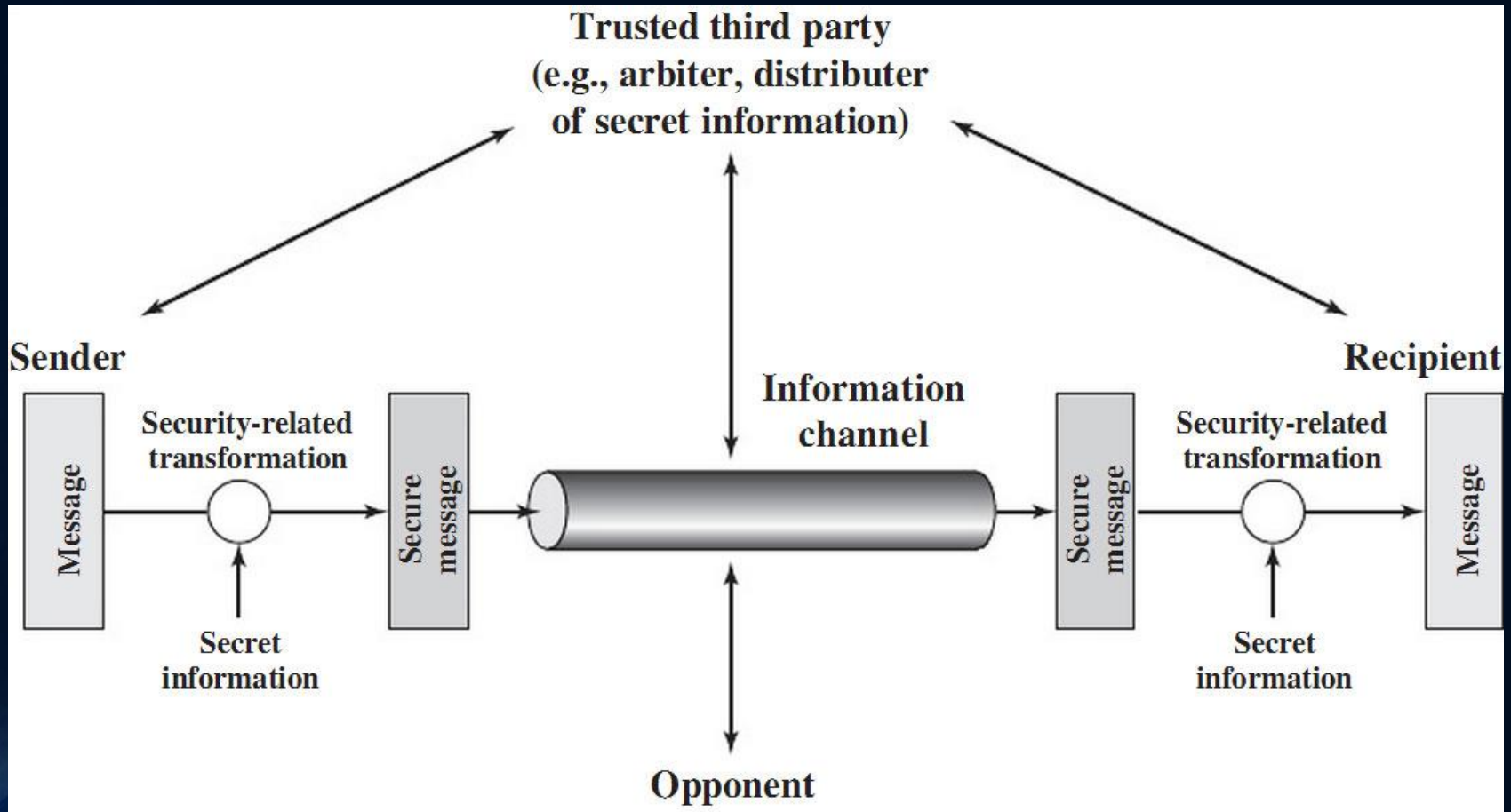


Figure 1.4 Model for Network Security

Model B for Security (Stallings, 2010)

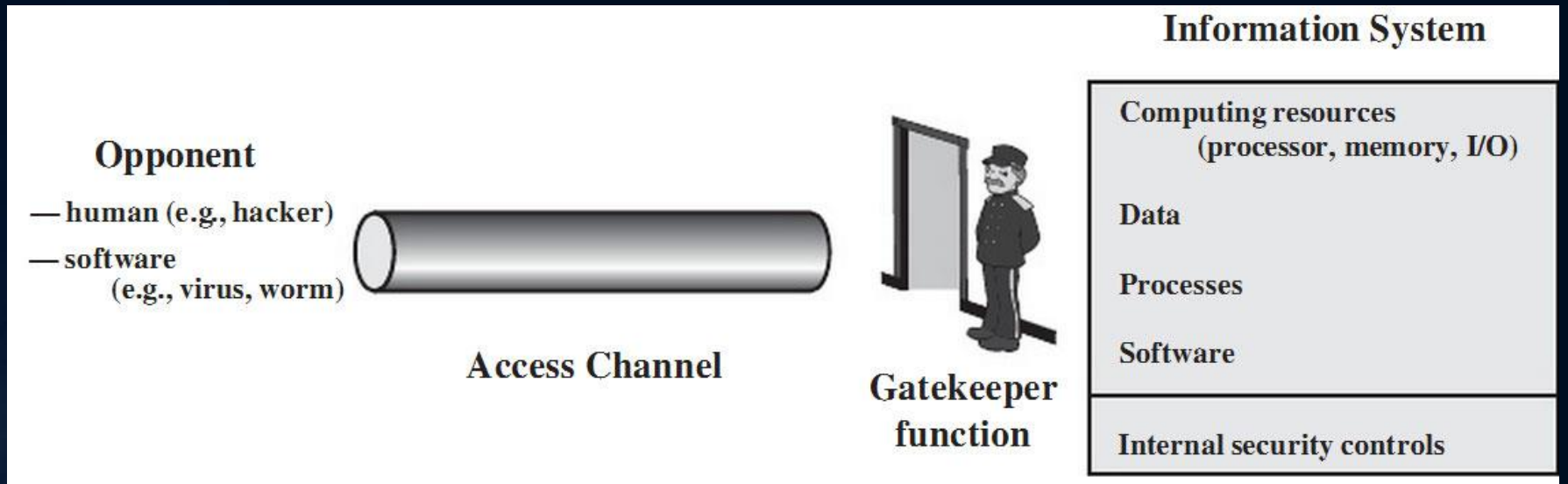


Figure 1.5 Network Access Security Model

Το Γνωστικό Αντικείμενο – 3η Θεώρηση

Πού γίνεται έρευνα:

MAY 20-23 AT THE WESTIN ST. FRANCIS, SAN FRANCISCO, CA

IEEE Symposium on Security and Privacy

Sponsored by the IEEE Computer Society Technical Committee on Security and Privacy in cooperation with the International Association for Cryptologic Research (IACR)

Co-located with the IEEE Computer Society Security and Privacy Workshops

Topics of interest include:

- Access control
- Accountability
- Anonymity
- Application security
- Attacks and defenses
- Authentication
- Censorship and censorship-resistance
- Distributed systems security
- Embedded systems security
- Forensics
- Hardware security
- Intrusion detection
- Language-based security
- Malware
- Metrics
- Network security
- Privacy-preserving systems
- Protocol security
- Secure information flow
- Security and privacy policies
- Security architectures
- System security
- Usability and security
- Web security

Το Γνωστικό Αντικείμενο – 2η Θεώρηση

Πού γίνεται έρευνα:

Overall, we are looking not only for solid results but also for some out of the box ideas. Areas of interest include (but are not limited to):

- Network perimeter controls: firewalls, packet filters, application gateways
- Network protocol security: routing, naming, network management
- Cloud computing security
- Security issues in Future Internet architecture and design
- Security of web-based applications and services
- Anti-malware techniques: detection, analysis, and prevention
- Secure future home networks, Internet of Things, body-area networks
- Intrusion prevention, detection, and response
- Combating cyber-crime: anti-phishing, anti-spam, anti-fraud techniques
- Privacy and anonymity technologies
- Security for wireless, mobile networks
- Security of personal communication systems
- Vehicular Ad-hoc Network (VANETs) Security
- Security of peer-to-peer and overlay network systems
- Electronic commerce security: e.g., payments, notarization, timestamping.
- Network security policies: implementation deployment, management
- Intellectual property protection: protocols, implementations, DRM
- Public key infrastructures, key management, certification, and revocation
- Security for Emerging Technologies
- Special problems and case studies: cost, usability, security vs efficiency
- Collaborative applications: teleconferencing and video-conferencing
- Smart Grid Security
- Secure Electronic Voting
- Security of large-scale critical infrastructures
- Trustworthy Computing for network protocols and distributed systems
- Network and distributed systems forensics

Το Γνωστικό Αντικείμενο – 2η Θεώρηση

Πού γίνεται έρευνα:

The 12th Privacy Enhancing Technologies Symposium (PETS 2012)

July 11–13, 2012

Vigo, Spain

Suggested topics include but are not restricted to:

- Anonymous communications and publishing systems
- Attacks on privacy and privacy technologies
- Censorship resistance
- Data protection technologies
- Economics of privacy and PETs
- Fielded systems and techniques for enhancing privacy in existing systems
- Location privacy
- Privacy and anonymity in Peer-to-Peer, Cloud, and Ubiquitous Computing Environments
- Privacy and inference control in databases
- Privacy-enhanced access control or authentication/certification
- Privacy-friendly payment mechanisms for PETs and other services
- Privacy in Online Social Networks
- Privacy policy languages and tools
- Privacy threat models
- Profiling and data mining
- Pseudonyms, identity management, linkability, and reputation
- Reliability, robustness and abuse prevention in privacy systems
- Traffic analysis
- Transparency enhancing tools
- Usability issues and user interfaces for PETs

Το Γνωστικό Αντικείμενο – 2η Θεώρηση

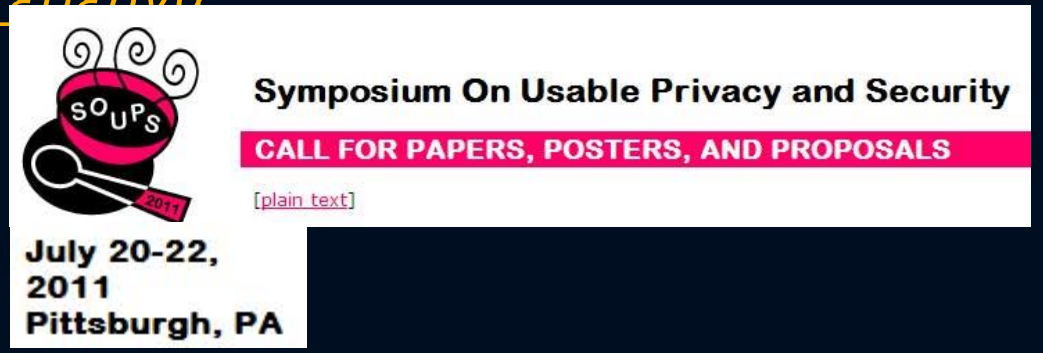
Πού γίνεται έρευνα;

esorics2012
pisa, italy – september 10-12, 2012

- access control
- accountability
- ad hoc networks
- anonymity
- applied cryptography
- authentication
- biometrics
- database security
- data protection
- digital content protection
- digital forensic
- distributed systems security
- electronic payments
- embedded systems security
- inference control
- information hiding
- identity management
- information flow control
- integrity
- intrusion detection
- formal security methods
- language-based security
- network security
- phishing and spam prevention
- privacy
- risk analysis and management
- secure electronic voting
- security architectures
- security economics
- security metrics
- security models
- security and privacy in cloud scenarios
- security and privacy in complex systems
- security and privacy in location services
- security and privacy for mobile code
- security and privacy in pervasive/ubiquitous computing
- security and privacy policies
- security and privacy in social networks
- security and privacy in web services
- security verification
- software security
- steganography
- systems security
- trust models and management
- trustworthy user devices
- web security
- wireless security

Το Γνωστικό Αντικείμενο – 2η Θεώρηση

Πού γίνεται έρευνα:



We invite authors to submit original papers describing research or experience in all areas of usable privacy and security.

- innovative security or privacy functionality and design,
- new applications of existing models or technology,
- field studies of security or privacy technology,
- usability evaluations of new or existing security or privacy features,
- security testing of new or existing usability features,
- longitudinal studies of deployed security or privacy features,
- the impact of organizational policy or procurement decisions, and
- lessons learned from the deployment and use of usable privacy and security features.

Το Γνωστικό Αντικείμενο – 2η Θεώρηση

Πού γίνεται έρευνα;

The Tenth Workshop on Economics of Information Security (WEIS 2011)

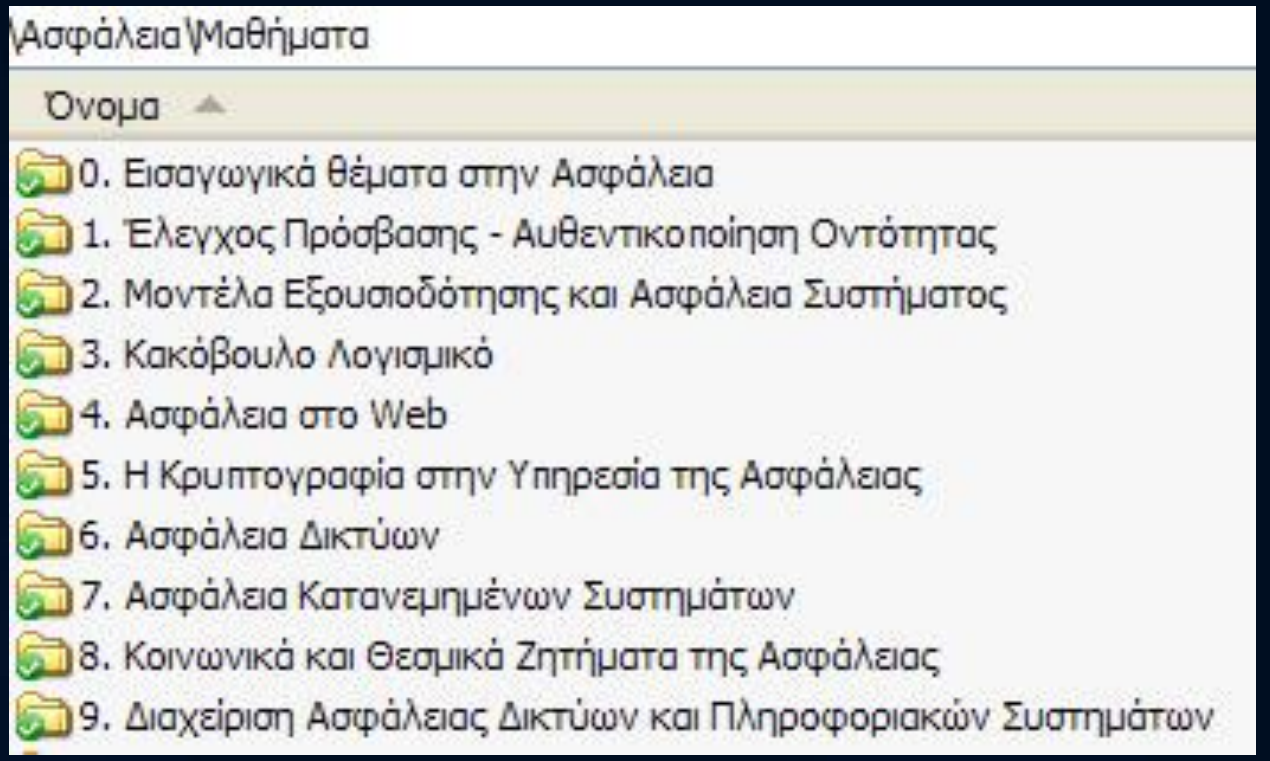
George Mason University, USA

June 14–15, 2011

- Optimal investment in information security
- Online crime (including botnets, phishing and spam)
- Models and analysis of online crime
- Risk management and cyberinsurance
- Security standards and regulation
- Cybersecurity policy
- Privacy, confidentiality and anonymity
- Behavioral security and privacy
- Security models and metrics
- Psychology of risk and security
- Vulnerability discovery, disclosure, and patching
- Cyberwar strategy and game theory
- Incentives for information sharing and cooperation

Το Γνωστικό Αντικείμενο – 3η θεώρηση

Ενοποίηση Θεμάτων Ασφάλειας (Τμήμα Πληροφορικής)



1. Έλεγχος Πρόσβασης (Access Control)

- Έλεγχος Λογικής Πρόσβασης:
  - Αυθεντικοποίηση Οντότητας
    - Passwords, CAPTCHA's, τεχνικές πρόκλησης – απάντησης, συστήματα ενιαίας πρόσβασης (single sign-on),…
- Έλεγχος Φυσικής Πρόσβασης
  - Αυθεντικοποίηση Οντότητας
    - Βιομετρία, smartcards, tokens…
  - Έλεγχος Φυσικής Πρόσβασης σε υποδομές και αγαθά

2. Μοντέλα Εξουσιοδότησης και Ασφάλεια Συστήματος

- ACLs, Ασφάλεια MLS and information flow
- Sandboxing & Virtualization
- Application Security
- Memory security
- File system Security
- Digital Forensics
- Database Security
- OS Kernel Security
- Trusted Computing
- Hardware Security
- Tempest and Side Channel Attacks
- Assurance and Evaluation

3. Κακόβουλο Λογισμικό

- Bots, Botnets
- Worms & Trojans
- Rootkits
- Spam, Phishing & Fraud
- Intrusion Detection
- Wireless & Cellular Malware
- …

4. Ασφάλεια στο Web

- Web browser security
- Web app & web server security
- Web privacy
- Web-based malware
- …

5. Η Κρυπτογραφία στην Υπηρεσία της Ασφάλειας

- Κρυπτογραφικές τεχνικές στην Ασφάλεια Επικοινωνιών & Δικτύων
- Προηγμένες τεχνικές αυθεντικοποίησης οντότητας και δεδομένων
- Κρυπτογραφικές τεχνολογίες εμπιστευτικότητας και ακεραιότητας
- Κρυπτογραφικές τεχνικές για την προστασία της ιδιωτικότητας
- Ασφάλεια και Ιδιωτικότητα σε Κατανεμημένες Εφαρμογές
- …

6. Ασφάλεια Δικτύων

- TCP/IP Security (Application, Transport, IP, MAC layers,…)
- Personal and Network Firewalls
- Penetration testing
- Network Authentication
- Network intrusion Detection
- Security in Wireless networks
- Network security policies
- …

7. Ασφάλεια Κατανεμημένων Συστημάτων

- Security Domains
- E-commerce transactions
- E-voting/ e-auctions
- Distributed Databases Security
- Distributed applications Security
- Distributed File Systems Security
- Web Services (WS) Security
- Security and Privacy in Pervasive Computing Environments
- Security and Privacy in Location-based Services (LBS)
- Security in banking/health sector

8. Κοινωνικά και Θεσμικά Ζητήματα της Ασφάλειας

- User anonymity & Privacy
- Freedom-of-Speech & Censorship
- Security and Usability
- Security Psychology
- Security Economics

- … Αλλά και:
  - Νομικά και Θεσμικά Ζητήματα
  - Κυβερνο-έγκλημα (Cyber crime)
  - Πνευματικά Δικαιώματα
  - Δεοντολογία & Κυβερνο-ηθική (Cyber-ethics)
  - …

9. Διαχείριση Ασφάλειας Δικτύων και Πληροφοριακών Συστημάτων

Published standards

- ISO/IEC 27000 — Information security management systems — Overview and vocabulary [1]
- ISO/IEC 27001 — Information security management systems — Requirements
- ISO/IEC 27002 — Code of practice for information security management
- ISO/IEC 27003 — Information security management system implementation guidance
- ISO/IEC 27004 — Information security management — Measurement
- ISO/IEC 27005 — Information security risk management
- ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27011 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27033-1 - Network security overview and concepts
- ISO 27799 - Information security management in health using ISO/IEC 27002 [standard produced by the Health Infomatics group

In preparation

- ISO/IEC 27007 - Guidelines for information security management systems auditing (focused on the management system)
- ISO/IEC 27008 - Guidance for auditors on ISMS controls (focused on the information security controls)
- ISO/IEC 27013 - Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001
- ISO/IEC 27014 - Information security governance framework
- ISO/IEC 27015 - Information security management guidelines for the finance and insurance sectors
- ISO/IEC 27031 - Guideline for ICT readiness for business continuity (essentially the ICT continuity component within business co
- ISO/IEC 27032 - Guideline for cybersecurity (essentially, 'being a good neighbor' on the Internet)
- ISO/IEC 27033 - IT network security, a multi-part standard based on ISO/IEC 18028:2006 (part 1 is published already)
- ISO/IEC 27034 - Guideline for application security
- ISO/IEC 27035 - Security incident management
- ISO/IEC 27036 - Guidelines for security of outsourcing
- ISO/IEC 27037 - Guidelines for identification, collection and/or acquisition and preservation of digital evidence

Βιβλιογραφία

- D. Gollmann. Computer Security. 3rd Edition, Wiley, 2011
- W. Stallings. Cryptography and Network Security, Principles and Practice. 5th Edition, Pearson, 2010
- R. J. Anderson. Security Engineering. 2nd Edition, Wiley, 2008
- S. L. Pfleeger. Security in Computing. 3rd Edition. Prentice Hall, 2003